UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,902	10/30/2001	Sanguthevar Rajasekaran	028410-0017	5784

29580 7590 03/08/2005

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
ATTN: JAN STEELE
525 UNIVERSITY AVENUE
SUITE 1100
PALO ALTO, CA 94301

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/015,902	Applicant(s) RAJASEKARAN ET AL..	
	Examiner Pramila Parthasarathy	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 August 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *4 and 8/2002*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on August 19, 2002. No preliminary amendments to the specification were filed. Claims 1 – 66 are currently being considered.

Specification

2. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

3. The following title is suggested: Access Control System with Camouflaging of Data and Information.

4. The disclosure is objected to because of the following informalities: Discontinuity in the subset.

Page 2 paragraph reads "The rest of the sub-objects (e.g., the subset {O_n, O_{n-1}, ... O_q}), ...", should be changed into "The rest of the sub-objects (e.g., the subset {O_n, O_{n+1}, ... Oq}), ... ".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

5. Claims 1, 2, 5 – 7, 10 – 12, 24, 26, 39, 42, 45, 48 and 51 – 66 are rejected under 35 U.S.C. 102(a) as being anticipated by Eldridge et al. (U.S. Patent Number 6,061,799).

6. Regarding Claims 1, 39, 51 and 55, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) representing in digital form a secret to be protected against unauthorized access (Column 4 lines 64 – Column 5 line 7);

(b) storing a plurality of computer-represented objects related to said secret (Column 4 line 64 – Column 5 line 7);

(i) at least one of said objects being accessible by an authorized user as a password (Column 5 lines 7 – 9);

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(c) representing said secret as a function of said plurality of objects, using a composition function (Column 5 lines 4 – 18 and 57 – 65); and

(d) storing, in a computer-readable memory, said composition function:

(i) in a manner accessible to said access control system (Column 8 line 63 – Column 9 line 13);

(ii) so as to be executable to generate a candidate secret using a user-inputted candidate password in conjunction with at least said another object stored in said wallet (Column 9 line 5 – 22);

(iii) said generated candidate secret not regenerating said secret if said candidate password is not said password (Column 9 lines 36 – 52), Eldridge teaches the key is generated only if the password is authorized; and

(iv) said generated candidate secret regenerating said secret if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 44);

thereby protecting said secret against unauthorized access by persons not having said password.

7. Regarding Claims 6, 42, 52 and 56, Eldridge teaches and describes a method for operating an access control system to release a secret camouflaged to be accessible to an authorized user yet protected against unauthorized access, said method comprising the steps of:

(a) accessing a plurality of computer-represented objects related to a secret (Column 7 lines 19 – 22);

(i) at least one of said objects being accessible by an authorized user as a password (Column 5 lines 7 –9);

(ii) at least another of said objects being stored in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(b) accessing a composition function representing said secret as a function of said plurality of objects (Column 9 lines 36 – 43);

(c) receiving a candidate password inputted by a user (Column 7 lines 8 – 10);

(d) generating a candidate secret for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said another object stored in said wallet (Column 5 line 56 – Column 6 line 11);

(i) said generated candidate secret not regenerating said secret if said candidate password is not said password (Column 9 lines 36 – 52), Eldridge teaches that the key is generated only if the password is authorized;

(ii) said generated candidate secret regenerating said secret if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 44); and

(e) outputting said candidate secret to said user of said access control system (Column 9 line 64 – Column 10 line 11).

8. Regarding Claim 11, 45, 53, 54, 57, 59, 60, 63 and 64, Eldridge teaches and describes a method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) obtaining state information represented in digital form (Column 5 lines 7 – 9 and Column 8 lines 15 – 19);

(b) deriving from said state information a first matrix (Column 5 lines 7 – 9 and Column 8 lines 19 – 24);

(c) storing said first matrix as a password usable by an authorized user (Column 4 line 64 – Column 5 line 7);

(d) deriving from said state information a second matrix (Column 5 lines 7 – 9 and Column 8 lines 15 – 19);

(e) storing said second matrix in a computer-readable wallet accessible to said access control system (Column 5 lines 7 – 9 and Column 8 line 63 – Column 9 line 13); and

(f) storing, in a computer-readable memory, a composition function executable to generate a candidate matrix using a user-inputted candidate password in conjunction with said second matrix (Column 9 lines 5 – 22);

(i) said generated candidate state information not regenerating said matrix if said candidate password is not said password (Column 9 lines 36 – 52), Eldridge teaches that the key is generated only if the password is authorized; and

(ii) said generated candidate state information regenerating said matrix if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 44);

thereby protecting said state information against unauthorized access by persons not having said password.

9. Regarding Claim 24, 48, 58, 61, 62, 65 and 66, Eldridge teaches and describes a method for operating an access control system to protect state information against unauthorized access, said method comprising the steps of:

(a) retrieving a first matrix related to said state information from a computer-readable wallet accessible to said access control system (Column 7 lines 19 – 22 and Column 8 lines 15 – 19);

(b) accessing a composition function representing said state information as a function of said first matrix and a password stored as a second matrix (Column 9 lines 36 – 43);

(c) receiving a candidate password inputted by a user (Column 7 lines 8 – 10);

(d) generating candidate state information for said user by executing said composition function using as operands thereto said candidate password in conjunction with at least said first matrix stored in said wallet ((Column 5 line 56 – Column 6 line 11 and Column 9 lines 5 – 22);

(i) said generated candidate state information not regenerating said state information if said candidate password is not said password (Column 9 lines 36 – 52), Eldridge teaches that the key is generated only if the password is authorized;

(ii) said generated candidate state information regenerating said state information if said candidate password is said password (Column 9 lines 36 – 52 and Column 10 lines 23 – 44); and

(e) outputting said candidate state information to said user of said access control system (Column 9 line 64 – Column 10 line 11).

10. Claims 2 and 12 are rejected as applied about in rejecting Claims 1 and 11. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, further comprising effecting a multilevel camouflaging scheme by camouflaging said at least another object stored in said wallet (Column 5 lines 56 – 67).

11. Claims 5 and 10 are rejected as applied about in rejecting Claims 1 and 11. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where:

(i) said secret is a private key of said user (Column 5 lines 18 – 22 and Column 6 lines 1 – 11);

(ii) said object accessible by said user is a PIN of said user (Column 5 lines 25 – 29);

(iii) said another object stored in said wallet is a pseudo-valid PIN (Column 7 lines 10 – 14); and

(iv) said candidate secret has the structural form of a private key (Column 5 lines 35 – 55).

12. Claim 7 is rejected as applied about in rejecting Claim 6. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where in said step (d)(i) said candidate secret is configured to deceive an unauthorized user into believing that said candidate secret is said secret (Column 5 lines 30 – 39).

13. Claim 26 is rejected as applied about in rejecting Claim 24. Furthermore, Eldridge teaches and describes a method for operating an access control system to camouflage a secret so as to be accessible by an authorized user yet protected against unauthorized access, where at least one of said matrices is stored on a smart card accessible to said user (Column 5 lines 4 – 14).

Claim Objections

14. Claims 3, 4, 8, 9, 13 – 23, 25, 27 – 38, 40, 41, 43, 44, 46, 47, 49 and 50 are objected to as being dependent upon a rejected upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. The following is a statement of reasons for the indication of allowable subject . matter:

Although, Eldridge teaches an access control system to camouflage a secret using a password and a secret parameter, Eldridge fails to particularly teach that said secret represents linkage information among nodes of a network and that secret represents at least one possible state of a system expressible as a Boolean logic function.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on Tuesday – Thursday 8:00a.m. To 3:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Pramila Parthasarathy
March 04, 2005.